DOI 10.37882/2223-2966.2025.07.20

ПЕРИОДИЧНОСТЬ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ, ПОСТРОЕННЫХ НА ВЫЧИСЛИТЕЛЬНОЙ МАШИНЕ

PERIODICITY OF RANDOM NUMBER GENERATORS BUILT ON A COMPUTING MACHINE

A. Kasyanov

Summary. In the context of exponential growth in cyber threats, the task of developing and analyzing pseudorandom number generators is becoming increasingly important. As of today, the relevance of the issue concerning finiteness of the period of generated sequences remains, due to the deterministic nature of the algorithms implemented on computing machines. Purpose of the study — to demonstrate the fundamental impossibility of constructing a generator with an infinite period based on a finite automaton, which is a mathematical model of a computing machine. The research is based on formal methods of finite automata theory, including the application of Kleene's theorem to establish equivalence between pseudo-random number generator algorithms and finite automata, and the theorem on the impossibility of recognizing non-periodic sequences, which justifies the finiteness of the period. The analysis performed in the framework of automata theory demonstrates that pseudorandom number generation algorithms can be implemented as finite automata, and are therefore subject to the limitation of the number of internal states and, consequently, the finiteness of the period of the generated sequence. Scientific novelty lies in the explicit application of theoretical results of finite automaton theory to justify the limitation of the period of pseudorandom number generators. The results obtained contribute to the understanding of the fundamental limitations imposed by the computing environment on the properties of generated sequences.

Keywords: algorithm, finite automata, regular expressions, non-periodic infinite sequences, Kleene's theorem, pseudorandom number generators.

Касьянов Александр Владимирович
Аспирант, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина);
Научный сотрудник отдела криптографического анализа, Специальный Технологический Центр (ООО «СТЦ»), г. Санкт-Петербург, Россия
kasjanov@inbox.ru

Аннотация. В условиях экспоненциального роста киберугроз, задача разработки и анализа генераторов псевдослучайных чисел приобретает исключительную актуальность. На сегодняшний день сохраняется актуальность вопроса, связанного с конечностью периода генерируемых последовательностей, обусловленный детерминированной природой алгоритмов, реализуемых на вычислительных машинах. Цель исследования — демонстрация принципиальной невозможности построения генератора с бесконечным периодом на основе конечного автомата, являющегося математической моделью вычислительной машины. Основу исследования составили формальные методы теории конечных автоматов, включая применение теоремы Клини для установления эквивалентности между алгоритмами генераторов псевдослучайных чисел и конечными автоматами, и теоремы о невозможности распознавания непериодических последовательностей, обосновывающей конечность периода. Проведенный анализ в рамках теории автоматов демонстрирует, что алгоритмы генерации псевдослучайных чисел реализуемы в виде конечных автоматов, а значит, подвержены ограничению числа внутренних состояний и, следовательно, конечности периода генерируемой последовательности. Научная новизна заключается в явном применении теоретических результатов теории конечных автоматов для обоснования ограниченности периода генераторов псевдослучайных чисел. Полученные результаты вносят вклад в понимание фундаментальных ограничений, накладываемых вычислительной средой на свойства генерируемых последовательностей.

Ключевые слова: алгоритм, конечные автоматы, регулярные выражения, непериодические бесконечные последовательности, теорема Клини, генераторы псевдослучайных чисел.

Введение

Сохраняющаяся дискуссия о конечности периода генераторов псевдослучайных чисел (ГПСЧ), реализованных на вычислительных платформах, определяет актуальность настоящего исследования. Несмотря на отдельные заявления о создании ГПСЧ с неограниченным периодом [1, 2, 3], в научной литературе, включая работы [4, 5, 6] и др., утвердилось представление о конечности периода всех ГПСЧ, построенных на детерминированных вычислительных машинах. Данное противоречие подчеркивает необходимость дальнейшего углубленного анализа теоретических ограничений, накладываемых архитектурой вычислительных машин на свойства генерируемых последовательностей, а также разработки строгих критериев оценки длины периода и методов ее максимизации в рамках существующих ограничений. Разрешение указанного противоречия имеет принципиальное значение для обеспечения надежности и безопасности криптографических приложений.

Последовательности случайных чисел играют значительную роль в генерации криптографических ключей,

инициализации криптографических алгоритмов, обеспечении анонимности и целостности данных [7]. Однако, несмотря на их широкое применение, получение псевдослучайных последовательностей с характеристиками эквивалентными «истинно» случайным последовательностям остается сложной задачей.

В настоящее время вследствие высокой стоимости и значительных массогабаритных характеристик аппаратных генераторов случайных чисел, генерация энтропии в большинстве случаев осуществляется программно, посредством алгоритмов.

В современной вычислительной математике и информатике понятие алгоритма является фундаментальным. «Алгоритм — описанная на некотором формальном языке точная конечная система правил, определяющая содержание и порядок действий над некоторыми объектами, строгое выполнение которых дает решение поставленной задачи» [8, С.7].

К ключевым характеристикам алгоритма относятся: «формальность, детерминированность, дискретностью, массовость, результативность» [8, С.8].

В данной работе будет исследован вопрос возможности построения ГПСЧ с бесконечным периодом, с точки зрения теории автоматов.

Конечные автоматы как абстрактные модели алгоритмических ГПСЧ

Для строгого обоснования ограничений на длину периода алгоритмических ГПСЧ, необходимо рассмотреть их представление в виде формальных моделей. Теория конечных автоматов предоставляет мощный инструмент для абстрактного описания вычислительных процессов. В данном разделе рассматриваются основные понятия теории конечных автоматов, а также доказывается теорема, устанавливающая принципиальную невозможность генерации непериодических последовательностей с помощью конечных автоматов. Этот результат имеет ключевое значение для понимания фундаментальных ограничений на период ГПСЧ, реализованных на вычислительных машинах.

Теорема. [9] Клини (совпадение классов автоматных и регулярных языков). Классы автоматных и регулярных языков совпадают. Т.е. любой регулярный язык является автоматным и любой автоматный язык является регулярным.

Дополнительно, в соответствии с [10] все реальные дискретные устройства, предназначенные для переработки информации, могут иметь только конечное число внутренних состояний (в виду ограниченности памяти устройств), т.е. их абстрактными моделями являются конечные автоматы.

Следовательно, каждый автоматный язык является регулярным множеством. «Для каждого регулярного выражения R может быть построен конечный автомат (возможно недетерминированный), распознающий выражение, задаваемое R» [9, С.17].

Поскольку конструкции алгоритмов программ могут быть описаны при помощи регулярных выражений, то согласно следствию из теоремы Клини алгоритм любой программы реализуем в виде конечного автомата.

Конечный автомат, как формальная модель в теории алгоритмов, представляет собой модель дискретного устройства с конечным числом состояний, входом и выходом. Входные воздействия и текущее состояние определяют выходной сигнал и следующее состояние. Различают детерминированные (ДКА), недетерминированные (НДА) и вероятностные (ВКА) конечные автоматы, характеризующиеся способом определения следующего состояния.

По теореме (о детерминизации) «для любого конечного автомата может быть построен эквивалентный ему детерминированный конечный автомат» [11, С.33]. Причем, «максимально возможное число состояний детерминированного автомата, полученного в результате детерминизации эквивалентного ему недетерминированного автомата, представленного m частными состояниями, не может быть больше, чем 2^m» [12, С.30] и определится из выражения:

$$M \leq \sum_{k=0}^{m} C_m^k = 2^m, \qquad (1)$$

где C_m^k — число сочетаний из m по k.

Максимальная длина периода псевдослучайной последовательности, генерируемой ГПСЧ, основанным на ДКА с m состояниями, не может превышать m. Следовательно, для ГПСЧ, представимого НДА с m частными событиями, верхняя граница длины периода составляет 2^m, поскольку это максимальное число различимых состояний, которое может быть достигнуто при развертывании НДА в ДКА.

В зависимости от структуры и функций переходов алгоритма [12], период ГПСЧ, на практике, может быть существенно меньше, чем верхняя граница, равная 2^m.

Определение. «Конечным автоматом называется система:

$$A = \left(S, X, Y, \delta, \lambda\right), \qquad (2)$$

где S — конечное множество состояний автомата; X, Y — конечные входной и выходной алфавиты соответственно, из которых формируются строки, считываемые и выдаваемые автоматом; $\delta : S \times X \to S$ — функция переходов; $\lambda : S \times X \to Y$ — функция выходов.

Если, кроме того, в автомате A выделено одно некоторое состояние, называемое начальным s_0, то полученный автомат называется инициальным» [13, С.295].

В отсутствие указанного начального состояния поведение автомата не детерминировано. Полное детерминированное описание автомата, согласно [13]:

$$A = \left(S, X, Y, \delta, \lambda, s_0\right). \quad (3)$$

Классификация конечных автоматов включает автоматы Мура, выход которых зависит лишь от внутреннего состояния, и автоматы Мили, выход которых определяется как внутренним состоянием, так и входным сигналом.

Лемма. «Для каждого конечного автомата Мили может быть построен эквивалентный ему конечный автомат Мура, и наоборот» [14, С.16].

На основании леммы, анализ возможностей автомата сводится к анализу автомата Мура. Представляя автомат Мура как автомат без выходов с классифицированными состояниями, возможно разделение состояний на два класса. Без потери общности автоматы можно переопределить, как автоматы без выходов [13]:

$$A = \left(S, X, \delta, x_1, F\right), \quad (4)$$

где $F \subseteq X$ — множество заключительных состояний, A — инициальный автомат без выхода с начальным состоянием x_1.

Событие (определение из теории грамматик) $E \subseteq S^*$ (S^* — множество слов (конечной длины) в алфавите S, включая пустое слово) представимо в автомате $A = \left(S, X, \delta, x_1, F\right)$, если $\delta\left(x_1, \alpha\right) \in F$, тогда и только тогда, когда $\alpha \in E$. Т.е. событие E — множество разрешимое в A.

Теорема. Конечные автоматы не способны распознавать непериодические бесконечные последовательности.

Доказательство (от противного). Предположим, непериодическая последовательность α распознаётся автоматом A с n состояниями. Тогда, по принципу Дирихле, при обработке α автомат повторит состояние, создавая цикл. Этот цикл позволяет построить периодическую последовательность α, распознаваемую в A, что противоречит не периодичности α и распознаваниюα автоматом A.

Полученное противоречие опровергает предположение о возможности распознавания непериодической последовательности конечным автоматом.

Следствие. Любой алгоритмический генератор случайных чисел, построенный на вычислительной машине, генерирует периодическую последовательность.

Анализ конечный автоматов с конечной памятью и их влияния на периодичность генераторов псевдослучайных чисел

В целях обеспечения более глубокого понимания вопроса исследовании в настоящем разделе представлены определения «систем с конечной памятью» [15, С.211], их представление конечными автоматами и теорема об оценке периодов генерируемых последовательностей.

Определение. «Системой с конечной памятью называется система, представимая конечным автоматом, в котором выходная реакция в любой дискретный момент времени зависит только от конечного ненулевого числа прошлых входных воздействий и от конечного числа прошлых выходных реакций.

Значит система с конечной памятью представима конечным автоматом, соотношение вход-выход которого может быть записана в форме» [15, С.211-212]:

$$y_v = g\left(x_{v-i_1}, x_{v-i_2}, \ldots, x_{v-i_u}, y_{v-j_1}, y_{v-j_2}, \ldots, y_{v-j_p}\right), \quad (5)$$

где y_v — выходной символ

Определение. «Конечный автомат, представляющий систему с конечной памятью, называется автоматом с конечной памятью» [15]. Таким образом, автомат с конечной памятью A, является автоматом, в котором

$$y_v = f\left(x_v, x_{v-1}, \ldots, x_{v-\mu_1}, y_v, y_{v-1}, \ldots, y_{v-\mu_2}\right), \quad (6)$$

где числа μ_1, μ_2 — называются соответственно x-памятью и z-памятью автомата A, а целое число $\mu = \max\left(\mu_1, \mu_2\right)$ называется максимальной памятью A.

Определение. «Линейный двоичный автомат — автомат с конечной памятью, входным и выходным алфавитом $\{0,1\}$ и выход в любой заданный момент времени равен сумме по модулю 2 ($\oplus$) значений выбранных входных символов в прошедшие моменты времени и выходных символов в прошедшие моменты времени» [15, С.227].

$$y_v = x_{v-i_1} \oplus x_{v-i_2} \oplus \ldots \\ \ldots \oplus x_{v-i_u} \oplus y_{v-j_1} \oplus y_{v-j_2} \oplus \ldots \oplus y_{v-j_p}, \quad (7)$$

где $0 \le i_1 < i_2 < \ldots < i_u$ и $1 \le j_1 < j_2 < \ldots < j_p$.

Теорема. «Пусть A — линейный двоичный автомат с памятью μ и -памятью μ. Тогда свободная выходная последовательность станет периодической не более чем через $2^{\mu'} + \mu - 1$ символов и ее период» [15, С. 233]:

$$\rho \le 2^{\mu'} - 1. \quad (8)$$

Следовательно, любая последовательность на выходе n-разрядного регистра сдвига с обратной связью всегда периодична, причем ее период:

$$\rho \le 2^n - 1. \quad (9)$$

Обсуждение

Вопрос о соотношении конечной природы вычислительных ресурсов и потенциальной бесконечности математических объектов, таких как число π или период ГПСЧ вроде Вихря Мерсенна (алгоритм, разработанный в 1997 году японскими учёными Макото Мацумото и Такудзи Нисимура) [16], затрагивает проблемы теории вычислений и прикладной реализации алгоритмов [17]. Алгоритм, способный вычислять число π или e с произвольной точностью, на первый взгляд, вступает в противоречие с концепцией конечного автомата или вычислительной машины с ограниченными ресурсами. Однако, кажущееся противоречие снимается при рассмотрении реализации бесконечных процессов в конечных системах посредством аппроксимации и ограничения точности вычислений [18].

Трансцендентность числа π обуславливает бесконечное непериодическое десятичное представление, что предполагает итеративный характер алгоритмов его получения. Несмотря на потенциальную бесконечность процесса вычисления, практическая реализация предполагает остановку после достижения целевой точности, необходимой для решения стоящей задачи или ограничениями, накладываемыми вычислительными ресурсами. Как было показано выше, алгоритм, представляет собой конечный набор инструкций и может быть реализован на конечной вычислительной машине. Бесконечность проявляется в потенциально неограниченном числе итераций, а не в структуре самого алгоритма. Поскольку потребность в абсолютной точности встречается редко, алгоритмы вычисления π включают критерий остановки, базирующийся на достижении заданной степени точности. Следовательно, вычисление числа π, несмотря на его теоретическую бесконечность, сводится к конечной аппроксимации, достаточной для конкретного приложения.

Вихрь Мерсенна — широко распространенный ГПСЧ, характеризующийся большим периодом ($2^{19937} - 1$). Несмотря на значительную величину периода, он является конечным, что подразумевает неизбежное повторение последовательности при достаточно продолжительной генерации. В отличие от истинной случайности, не демонстрирующей детерминированных закономерностей, псевдослучайность представляет собой детерминированный процесс, моделирующий свойства случайности. Следовательно, период любого ГПСЧ конечен.

Необходимо отметить, что даже при периоде ГПСЧ, превосходящем оценочное число атомов во Вселенной, такой генератор не может рассматриваться как идеально случайный. Так как все ГПСЧ демонстрируют статистические отклонения и закономерности, выявляемые специализированными статистическими тестами, например «Стопка книг». Вихрь Мерсенна не предназначен для получения криптографически стойких случайных последовательностей чисел.

Выбор ГПСЧ должен основываться на строгом соответствии требованиям конкретной задачи, подкрепленном детальным анализом его статистических характеристик. Критически важным параметром, определяющим степень непредсказуемости и пригодности ГПСЧ для использования в криптографических приложениях, является оценка энтропии генерируемой последовательности. Низкая энтропия может свидетельствовать о скрытых корреляциях, компрометирующих надежность ГПСЧ.

Заключение

В настоящей работе исследованы ограничения, накладываемые теорией конечных автоматов на алгоритмические ГПСЧ. Проведен строгий теоретический анализ, основанный на применении теоремы Клини и теоремы о невозможности распознавания непериодических последовательностей конечными автоматами для строгого обоснования принципиальной ограниченности периода ГПСЧ, который демонстрирует, что детерминированная природа алгоритмов, реализуемых на вычислительных машинах, формализуемых в виде конечных автоматов, неизбежно приводит к конечности периода генерируемых псевдослучайных последовательностей.

Осознание принципиальной ограниченности периода ГПСЧ критически важно при выборе подходящего ГПСЧ для криптографических приложений (генерация ключей, потоковое шифрование и др.). Необходимо выбирать ГПСЧ с максимально возможным периодом (близким к теоретической границе), чтобы избежать риска повторения ключевой последовательности и компрометации системы шифрования.

Результаты исследования могут быть использованы при разработке гибридных генераторов, сочетающих несколько ГПСЧ, для увеличения общей длины периода и повышения криптографической стойкости. Понимание ограничений каждого отдельного ГПСЧ помогает строить более надежные и эффективные алгоритмы, способные приближаться к теоретической границе по длине периода при сохранении высокой производительности и криптографической стойкости. Также результаты могут быть полезны для анализа безопасности и обоснования рекомендаций по выбору существующих ГПСЧ (например, используемых в операционных системах, криптографических библиотеках) для различных приложений с учетом требований к безопасности и производительности.

ЛИТЕРАТУРА

1. Kalyanov, K. Random number generator based on the standard mapping / K. Kalyanov // Colloquium-Journal. — 2019. — No. 12-2(36). — pp. 67–68. URL: https://www.elibrary.ru/item.asp?id=38317591 (дата обращения: 06.06.2025).
2. Koranne, Advay. Non-Periodic Pseudo-Random Number Generator Using Sinai Billiards. Washington, DC: Society for Science — 2019. URL: https://abstracts.societyforscience.org/Home/FullAbstract?ProjectId=18805
3. Кренделев, С.Ф. Генераторы псевдослучайных чисел, не имеющие периода / С.Ф. Кренделев, А.Ю. Кузьменок // Математические заметки СВФУ. — 2014. — Т. 21, № 4. — С. 31–38. — EDN UISITV. URL: https://www.elibrary.ru/download/elibrary_24160562_27528359.pdf (дата обращения: 06.06.2025).
4. Мирзоян, С.А. Критерии качества и распространенные ошибки разработки генераторов псевдослучайных чисел / С.А. Мирзоян // Вестник современных цифровых технологий. — 2024. — № 21. — С. 44–48. — EDN LMHBHD. URL: https://www.elibrary.ru/item.asp?id=78472480 (дата обращения: 06.06.2025).
5. Нечаев, К.А. Исследование способов формирования псевдослучайных чисел с большим периодом / К.А. Нечаев, М.А. Орлов, Н.А. Иванов // Наука и бизнес: пути развития. — 2022. — № 1(127). — С. 19–27. — EDN TPCUFP. URL: https://www.elibrary.ru/item.asp?id=48219985, (дата обращения: 06.06.2025).
6. Вопросы построения программных систем оценки качества стохастических алгоритмов / А.О. Прокофьев, И.В. Чугунков, Е.А. Матрюхина, Е.А. Гриднева // Современные информационные технологии и ИТ-образование. — 2016. — Т. 12, № 3-1. — С. 169–178. — EDN XBWGUR. URL: https://www.elibrary.ru/item.asp?id=27411989, (дата обращения: 06.06.2025).
7. Grishentsev A.Yu., Arustamov S.A., Korobeynikov A.G., Kozin O.V. Orthogonal noise-like signal symbols for broadband channel protection. Scientific and Technical Journal of Information Technologies, Mechanics and Optics, 2019, vol. 19, no. 2, pp. 280–291 (in Russian). DOI: 10.17586/2226-1494-2019-19-2-280-291, (дата обращения: 06.06.2025).
8. Бочарова, Т.А. Основы алгоритмизации: учебное пособие / Т.А. Бочарова, Н.О. Бегункова; М-во образования и науки Российской Федерации, Гос. образовательное учреждение высш. проф. образования «Тихоокеанский гос. ун-т». — Хабаровск: Изд-во ТОГУ, 2011. — 63 с.: ил.; 21 см.; ISBN 978-5-7389-0966-5. — Текст: непосредственный.
9. Мастихина А.А. Формальные языки и автоматы [Электрон. ресурс]: метод. указ. к выполнению домашнего задания по дискретной математике / Мастихина А.А.; ред. Исмагилов Р. С. // МГТУ им. Н.Э. Баумана. — М.: Изд-во МГТУ им. Н. Э. Баумана, 2011. — 23 с. URL: http://hoster.bmstu.ru/~fn1/wp-content/uploads/2011/08/uchebno-metod/Mastihina_Form_yaz_Avt.pdf. (дата обращения: 06.06.2025).
10. Энциклопедия кибернетики: [в 2 т.] / Акад. наук Укр. ССР; редкол.: В.М. Глушков (отв. ред.) [и др.]. — Киев: Главная редакция Украинской Советской Энциклопедии, 1974. — 3агл. обл.: ЭК. — Текст: непосредственный. Т. 1: Абс-Мир. — 1974. — 608, [1] с.: ил., табл., [5] л. цв. ил.; 24 см. — (впер.): Б.ц.
11. Касьянов, В.Н. Лекции по теории формальных языков, автоматов и сложности вычислений: [учебное пособие для студентов-математиков и информатиков] / В.Н. Касьянов; Гос. ком. Рос. Федерации по высш. образованию, Новосиб. гос. ун-т Новосибирск: Редакционно-издательский отдел НГУ, 1995, 112 с.: ил. — Текст: непосредственный.
12. Вашкевич, Н.П. Недетерминированные автоматы и их использование для реализации систем параллельной обработки информации: моногр. / Н.П. Вашкевич, Р.А. Бикташев. — Пенза: Изд-во ПГУ, 2016. — 394 с. ISBN 978-5-906831-93-4. — Текст: непосредственный.
13. Кузнецов, О.П. Дискретная математика для инженера / О.П. Кузнецов, Г.М. Адельсон-Вельский — [2-е изд., перераб. и доп.]. — М.: Энергоатомиздат, 1988. — 479, [1] с. ил.; 22. — ISBN 5-283-01563-7. — Текст: непосредственный.
14. Гуренко, В.В. Введение в теорию автоматов [Электронный ресурс]: электронное учебное издание: учебное пособие по дисциплинам «Теория автоматов», «Прикладная теория цифровых автоматов» / В.В. Гуренко; Московский гос. технический ун-т им. Н.Э. Баумана, Фак. «Информатика и системы управления», Каф. «Компьютерные системы и сети». — Москва: МГТУ им. Н.Э. Баумана, 2013. — URL: https://e-learning.bmstu.ru/iu6/pluginfile.php/2978/mod_data/content/1282/bmstu_IU-6_automates_theory.pdf, (дата обращения: 06.06.2025).
15. Гилл, Артур. Введение в теорию конечных автоматов / Пер. с англ. А.Т. Дауровой [и др.]; Под ред. П.П. Пархоменко. — Москва: Наука, 1966. — 272 с.: черт.; 21 см. — (Теоретические основы технической кибернетики). — Текст: непосредственный.
16. Makoto Matsumoto, Takuji Nishimura. 1998. Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator. ACM Trans. Model. Comput. Simul. 8, 1 (Jan. 1998), 3–30. https://doi.org/10.1145/272991.272995
17. Поляков, В.И. Основы теории алгоритмов: учебное пособие / В.И. Поляков, В.И. Скорубский. — Санкт-Петербург: НИУ ИТМО, 2012. — 51 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/43564 (дата обращения: 07.06.2025). — Режим доступа: для авториз. пользователей.
18. Кнут, Д.Э. Искусство программирования, т. 2. Получисленные алгоритмы, 3-е изд.: Пер. с англ. — СПб.: ООО «Диалектика», 2020. — 832 с.: ил. — Парал. тит. англ. — ISBN 978-5-907144-15-6. — Текст: непосредственный.